أسرارك و هويتك الإلكترونية معروضة في ميدان عام





إحذر: هويتك مفضوحة عند زيارة مواقع الويب (جزء ٢)

في العدد الماضي تعرضنا لموضوع «الهوية على الإنترنت» .. وكيف أنه منذ اللحظة الأولي التي تقوم فيها بالولوج علي الإنترنت..فإنك تقدم معلومات سهلة للعالم كله تكشف عن شخصيتك..بل وماذا تفعل الآن علي الشبكة.
فمن المعروف أن أجهزة الحاسب التي تكون شبكة الإنترنت تراقب تحركاتك وتقوم بتسجيلها لحظة بلحظة بمجرد ولوجك.
وكذلك تعرضنا للطريقتين التين يمكن خلالهما الحصول على معلومات عنك .. فتطرقنا إلي الطريقة الصريحة والتي يتم الحصول علي معلومات عنك خاصة باسمك وعنوانك ورقم هاتفك وعنوان البريد الإلكتروني الخاص بك.. إلخ.. عن طريق (إجبارك) علي تقديم هذه المعلومات فيما يسمي بعملية «التسجيل» لدي الموقع والتي بدونها لن تستطيع الدخول أو حتي الحصول علي معلومات من الموقع نفسه أو استخدام الخدمة التي يقدمها هذا الموقع .. و بمجرد تقديم بياناتك يقوم بعد ذلك الموقع بعملية (بيع) لهذه المعلومات لشركات التسويق التي تطوق لمعرفة اتجاهاتك التسويقية وطباعك التي قد تفيد الحملات التسويقية لها.

أيضا هناك العديد من الطرق الضمنية التي تتيح للمواقع معرفة العديد من المعلومات و(التصرفات) عنك عند ولوجك علي أحدهم .. كان أهم هذه الطرق هي إستخدام الكوكيز Cookies.. فلفظ كوكيز يمثل عدة أسطر مكونة من 256 حرف مشفرة يقوم بتخزينها الموقع علي حاسبك والتي يمكن للموقع إستدعائها فيما بعد.. وعادة ما تتكون هذه المعلومات من اسم الموقع .. متي كانت آخر زيارة لك؟ من أين قمت بهذه الزيارة؟ ما هي الصفحات التي دخلت عليها بالموقع في آخر زيارة لك؟ وكم من الوقت قضيت داخل كل صفحة؟

أيضا معرفة هويتك عبر رسائلك المرسلة بالبريد الإلكتروني لتعد طريقة ثالثة حيث أن الرسالة لا تصل مباشرة منك إلى هذا الشخص بل تنتقل من حاسب إلي حاسب في رحلتها عبر شبكة الإنترنت إلي أن تصل إلي هدفها.. وبالتالي يمكن لأي شخص بواسطة تجهيزات بسيطة (إصطياد) هذه الرسائل أثناء مرورها عليه في رحلتها.
أيضا تواجد الرسالة علي صندوقك البريدي لدي مزود الخدمة لحين «سحبها» والإحتفاظ بها علي حاسبك لهي مشكلة أخري.. فأحد الموظفين في «الوردية الليلية (أو النهارية) لمزود خدمة الإنترنت ISP يمكن أن «يتسلي» بقراءة محتويات صندوقك لقتل الوقت.

في هذا العدد و بعد أن استعرضنا ما سبق تفصيليا في العدد الماضي .. سنستعرض معاً الطرق المختلفة التي يمكنك من خلالها القيام بعمل حاجز منيع ضد التعدي علي خصوصياتك وهويتك علي الإنترنت.
1. إسأل عن سياسة الخصوصية (Privacy Policy) للموقع: –
نتيجة للضغط الإعلامي والإهتمام الدولي بهذه القضية فلقد قامت العديد من المواقع ومزودي خدمة الإنترنت بعمل وثيقة تحدد فيها سياساتهم تجاه البيانات المنشورة لديهم.
في هذه الوثيقة ستجد نوعية المعلومات التي يقومون بجمعها عنك وكذا الإتجاهات التي سيتم إستخدامها فيهم.
للأسف لم نجد في أى موقع عربي هذه الوثيقة أو ما يفيد وجود سياسة خصوصية لديهم.
أما عن موقعنا http:// www.internet.com فسياسة الخصوصية فيه واضحة ة يمكنك أن تجدها في العنوان التالي: http://www.internet.com/corporate/privacy/privacypolicy.html

2. لا تقدم بياناتك الحقيقية عند



التسجيل لدي موقع ما :
هل يملك الموقع وثيقة خاصة بالخصوصية؟؟ لو كانت الإجابة بنعم.. فإن تسجيل بياناتك داخل الموقع (من المحتمل) أن يكون آمنا.
أما لو لم تجد فإنه بالتأكيد سيمكنك البحث عن بيانات الموقع لدى آخر لا يطلب منك التسجيل.
تذكر أيضاً أنه بإستثناء تقديم معلومات مثل الخاصة ببطاقة الإئتمان عند الشراء من مواقع مؤمنة (Secured).. فإنه يمكنك تقديم معلومات خاطئة وغير حقيقية عن نفسك.
فعنوان مثل «1234 شارع» سيتم قبوله من معظم مواقع الويب وكأنه عنوانك الحقيقي.

3. تتبع إستخدام إسمك:
في المرات القادمة عند تسجيلك لدى إي من المواقع إستخدم أسماء مختلفة أو تغيير طفيف في إسمك وليكن إضافة رقم مختلف بجوار الإسم الأول مع تدوين كل إسم والموقع الذي سجلته فيه.
إذا قمت بعد ذلك بإستلام رسائل إلكترونية معنونة بأحد هذه الأسماء فإنه سيمكنك معرفة ما هو الموقع الذي باع بياناتك حيث يمكنك مخاطبته بل ومقاضاته إذا أردت.

4. إحتفظ بعنوان بريد إلكتروني إضافي:
يمكنك مجانا الحصول علي عنوان بريد إلكتروني جديد لدي أحد المواقع المجانية مثل Hot Mail (www.hotmail.com) أو usa.net (www.usa.net) يمكنك بعد ذلك إستخدام هذا العنوان البريدي المجاني في أي عملية تسجيل لدي أي موقع وبالتالي تضمن عدم إستخدام عنوان البريد الإلكتروني الأصلي الخاص بك.
سيجب عليك بعد ذلك قراءة البريد من هذا العنوان الثانوي لتتبع الرسائل التي تأتي إليك من خلاله بصفة دورية كل أسبوع مثلاً.

5. إستخدم موقع (بدون هوية Anonymizer):
موقع http:// www.anonymizer.com هو موقع «وسيط» يعمل كحلقة وصل بين متصفحك وبين مواقع الويب الأخري.. كما يمنع هذه المواقع من الحصول علي أي معلومات خاصة بك.

لكي تقوم بإستخدام هذه الخدمة.. يمكنك أن تقوم بإضافة الكلمات التالية قبل كتابة عنوان أي موقع تقوم بزيارته (http://www.anonymizer.com:8080).
فمثلا لزيارة موقعنا arabia.internet.com يمكنك كتابة ذلك كالتالي:
http://arabia.internet.com./http://www.anonymizer.com:8080.
العيب الوحيد لخدمة anonymizer أنها تضيف مرحلة جديدة في رحلة المعلومات للوصول إلي متصفحك.. حيث أن قبل وصول البيانات إلي متصفحك يقوم موقع anonymizer بتلقي هذه المعلومات بدلاً من متصفحك ثم إعادة إرسالها إليك بعد ذلك في الحال مما يبطئ عملية وصول المعلومات إليك.
أيضاً لزاماً عليك أن تقوم بإضافة الجملة السابقة قبل أي موقع ويب ستقوم بزيارته.

إذا كنت قد قررت بالفعل الإعتماد علي موقع anonymizer بصفة دائمة فإنه يمكنك بكل بساطة ضبط متصفحك لكي يقوم بإضافة هذه الكلمات عنك لأي موقع ويب تود زيارته.
لتفاصيل أكثر عن هذا يمكنك زيارة موقع anonymizer الويب: http://www.anonymizer.com.

6. منع ال Cookies من وضع نفسها علي حاسبك الشخصي:
معظم الإصدارات الحديثة من متصفحي الإنترنت Internet browsers مثل نيتسكاب و إكسبلورار تسمح لك بالتحكم في عملية السماح أو منع مواقع الإنترنت من وضع الكوكيز علي حاسبك.
سنقوم بعد قليل بإعلامك عن الكيفية التي يمكنك بها التحكم في ذلك في كلاً من المتصفح نيتسكاب الاصدار الرابع وكذا إنترنت إكسبلورار الاصدار



أسرارك مشاع للجميع

الخامس.
أيضاً برنامج مثل PGP Cookies قد يمكنه حل هذه المشكلة لك حيث يقوم بالتحكم للسماح لبعض المواقع بعينها بإضافة الـcookies بينما يقوم بمنع مواقع أخرى معينة من وضع الcookies الخاصة بها.

فموقع مثل cnn.com أو Amazon.com قد يكون من المفيد لك أن يحصلا علي معلومات عنك من أجل »تفصيل« الأخبار التي تهمك أو إعلامك بالجديد في نوعية الكتب التي تستهويك بينما موقع آخر مثل www.net-hacking.com لمن المفضل عدم السماح له بعمل ذلك.

أيضاً حل آخير لكي تعيش بدون cookies هي أن تقوم بحذفها بإستمرار من خلال الدخول folder الويندوز المسمى Internet temporary files من داخل c:// windows وحذف ملفات الـ Cookies بصفة مستمرة (أنظر الصورة التي تمثل شكل ملفات ال cookies داخل الfolder المذكور) .. أو من خلال ال utility مثل الموجودة بالقرص المدمج لهذا العدد.

فقط يجب أن نذكر أنه بدون وجود Cookies فإن المواقع التي تقوم بتفصيل المعلومات طبقاً لرغبتك مثل amazon.com مثلاً التي تقوم بإقتراح كتب جديدة طبقاً لإختياراتك في آخر زيارة لك للموقع عند قيامك بزيارة الموقع من جديد.فإنها لن تستطيع القيام بذلك.

7. إستخدام موقع البريد الإلكتروني بدون هوية: –
تسمح لك هذه المواقع بإرسال أي رسالة بريد إلكتروني إليها حيث تقوم هي بحذف كل ما يحص عنوانك البريدي أو أي معلومات أخري مرفقة ببريدك الإلكتروني مثل مزود الخدمة الخاص بك و المسار التي سارت فيه الرسالة... إلخ.. ثم إعادة إرسال هذه الرسالة تحت عنوان مشابه لعنوان an1254@nowhere.net دون أي إشارة لعنوانك الحقيقي.

كل مواقع البريد الإلكتروني بدون الهوية تقدم خدماتها بالمجان و لكن ما يعيب هذه الطريقة هو أنها لن تسمح بإستقبال أي ردود علي رسالتك وبالقاء وتصلح فقط للاشتراك في خدمة ما أو التنويه عن خبر ما دون أن يكون في نيتك تلقي أي ردود من مستقبلي الرسالة.
أيضا بعض الناس قد يثير قلقهم وصول رسالة ما إلي صندوقهم بدون معرفة هوية المرسل وبالتالي قد لا تؤدي الرسالة الغرض منها.
8. إستخدم خاصية التشفير: –
أفضل طريقة لمنع الهاكرز من قراءة بريدك الإلكتروني هو إستخدام خاصية التشفير.. فقط عليك أن تتأكد أن الطرف الآخر الذي سيقوم بإستلام الرسالة لديه نفس برنامج فك الشفرة الذي قمت أنت بإستخدامه لتشفير رسالتك.. وبالتالي يصلح هذا الأمر لإرسال و استقبال الرسائل بين أفراد هيئة أو شركة معينة أخر بين أصدقاء متفق بينهم إستخدام نفس النسخة.. ولا يصلح بالطبع كأسلوب تقليدي لإرسال رسائلك لغير هؤلاء.

في النهاية فإن الإنترنت ستظل دائماً مكانا »مفتوحا« للبيانات.. كذلك كم المعلومات عنك التي يجب السماح للغير بالوصول إليها ما يزال سؤال بلا إجابة محددة.. فلا توجد بعد أي قوانين تحكمها.

إن حماية خصوصيتك علي الويب هي شيئا لابد أن تقوم بعمله بيديك أنت.. فعن طريق معرفة بعض الطرق الخفية لحصول البعض على معلومات عنك .. سيجعل بالإمكان أن تقوم بعمل التحصين الدفاعي اللازم لذلك.

أما قوة هذا التحصين الدفاعي فهي تبعاً لقرارك عن مدي الخصوصية التي ترغبها عند تجوالك علي الإنترنت وكذا المجهود الإضافي الذي »ستضطر« للقيام به للحصول علي هذه الخصوصية المفقودة.

تعليق على مقال العدد السابق بقلم: القارئ طارق قاسم

وجد على شبكة إنترنت عدة مواقع تؤمن لك سرية تحركاتك.

فموقع: www.anonymizer.com مثلا يوفر لك من خلال خدمة (Anonymizer Surf) إمكانية إخفاء هويتك عن المواقع التي تزورها ..حيث يتسلم اسم الموقع الذي ترغب في زيارته و يوصلك إليه بدون أن يمكنه من تسجيل أي معلومات عنك حيث سيبدو للموقع الذي تزوره أنك قادم من عنوان IP الخاص بموقع (أنونيمايزر)حيث تشفر هذه الخدمة كل تصرفاتك على الشبكة باستخدام تقنيات تشفير متطورة (128بت) مما يضمن لك سرية إرسال البريد الإلكتروني والدردشة عبر الإنترنت و إخفاء هويتك حتى عن مزودي خدمات إنترنت ISP وتقدم هذه الخدمة إما مجانا بسرعة بطيئة نسبياً أو لقاء 40 دولار كل 3 اشهر مع سرعة ممتازة ومزايا افضل ... وهي تشبه في ذلك طاقية الإخفاء...ستلاحظ ذلك عندما تدخل الموقع.

موقع آخر شهير في هذا المجال هو : WWW.ULTIMATE-ANONYMITY.COM حيث يقدم هذا الموقع خدماته بأسعار زهيدة جدا تبلغ 14دولار تدفع مرة واحدة فقط وهو مشهور جدا في الأمان والسرية .

بالنسبة لبرامج السرية والأمان في الإنترنت هناك برنامج اسمه GHOST MAIL تستطيع جلبة مجانا من الموقع WWW.ER.UQAM.CA/MERLIN./FG591543/gm حيث يوفر لك إمكانية إرسال رسائل إلكترونية بدون الكشف عن العنوان IP الخاص بكمبيوترك أو بالكمبيوتر المتصل. أيضا هناك برنامج آخر اسمه FREEDOM تستطيع جلب إصدارة SHAREWARE تجريبه مجانية صالحة لمدة 30يوم من الموقع WWW.ZEROKNOWLEDGE.COM حيث يستخدم عملية تشفير 128بت . و مبدأ عمله انه يسمح لك باستخدام اسما مستعارا لتصفح الشبكة وإرسال البريد الإلكتروني والدردشة والمشاركة في مجموعات الأخبار والقوائم البريدية كما يتيح لك التحكم في إعداد المعلومات التي ستكشفها مواقع انترنيت عن (هويتك الرقمية المستعارة). وهذا البرنامج يتضمن دعما لثلاثة أسماء مستعارة بثلاثة هويات رقمية (معلوماتك شخصية) مستعارة .. لكن إذا أردت الحصول على الإصدار كاملا فانه سيكلفك 50 دولارا ويمكنك من استخدام خمسة أسماء مستعارة كل اسم مستعار لمدة عام حيث يسمح لك البرنامج بالتحكم فعليا بما تريد أو لا تريد من السكاكر COOKIES تحت كل اسم مستعار.

أيضا يمكنك أن تقوم بتجربة موقع WWW.PRIVACYX.COM الذي يقدم خدماته مجانا بالكامل:

-بريد مجاني مشفر ومتخف.
-تصفح مجاني مشفر و متخف.
-دردشة مجاني مشفر ومتخف.

كما تجد في موقع WWW.PRIVACY.NET/SOFTWARE برامج يمكنك جلبها لكي تمحو ما سجل في كمبيوترك عن نشاطاتك في الانترنيت من COOKIES,CACHES,HISTORY FILES,NEWSGROUP ARCHIVES....

و هناك آخر هو: www.webtrends.net/tools/security/scan.asp يجري عملية فحص لجهازك و يكشف مواطن الخلل فيه التي تتيح للمتطفلين اختراقه و يدلك على أنجح الطرق لحمايته و يرسل لك النتائج بالبريد الإلكتروني. و هذا البرنامج يمكنك جلبه من الموقع السابق مجانا لمدة 14 يوم أو نسخة كاملة بسعر ما بين 150 و 5000 دولار حسب نوع الخدمات المضافة .

و أخيرا هنالك موقع : www.ziplip.com لحماية بريدك الإلكتروني من المتلصصين Web Based E-mail

و موقع www.hushmail.com الذي يوفر درجة تشفير تصل إلى 1024 بت للبريد الإلكتروني.

بقيت ملحوظة يجدر الإشارة اليها هي أن الجهة الوسيطة



التي تقدم لك تلك الخدمات تحتفظ بسجل عن كافة تحركاتك .لكنها لا تكشفه لأحد حفاظا على سمعتها الأمنية-إلا في حال وقوع اعتداء معين مصدره الحاسوب الذي تستخدمه(كالقرصنة).

وهنالك أيضا مشكلة أخرى هي أن الخدمات السابقة مثل Anonymizer تسمح بتصفح المواقع التي يمنعها البروكسي Proxy ويحتمل لهذا السبب أن يمنع بعض مزودي خدمات الإنترنت ISP في البلدان العربية ة خاصة السعودية الوصول إلى مثل تلك المواقع.

كلمة أخيرة : هنالك ما يسمى بالسكاكر Cookies والتي تفيد في تسريع وتسهيل الدخول للمواقع التى زرتها سابقا كما ذكر تفصيليا في مقال العدد الماضي .. ويمكنك التحكم فيها كما سيلي:

-اختر الأمر View من شريط الأدوات العلوي لمتصفحك بالنسبة ل IE4 .

-اختر Internet Options خيارات انترنت .

-اختر Advanced خيارات متقدمة.

– تحرك بالزالق Scroll bar للأسفل حتى تصل للخيار Cookies

فتظهر لك 3 خيارات هي:

1/القبول المباشر Accept cookies .

2/طلب الأذن منك Ask me before accept cookies.

3/إبطال فعلها Disable cookies.

واختر منها ما تحب .

ملاحظة: بالنسبة لIE5 تتبع ما يلي :

-اختر الأمر Tools من شريط الأدوات العلوي لمتصفحك.

-اختر Internet Options .

-اختر لسان التبويب Security وانقر على الزر Custom level فيظهر مربع حوار اختر منه الزر Settings.

-فيظهر مربع جديد ..حرك الزالق للأسفل حتى تصل للخيار Cookies واختر ما تحب منها.

بالنسبة لمستخدمي نيتسكاب .. يمكنكم اتباع الآتي:

– اختر الأمر Edit من شريط الأدوات العلوي لنيتسكاب.

– إختر أمر preferences خيارات.

– أختر أمر advanced متقدم (في نهاية القائمة).

– حدد ماذا تريد من الخيارات الثلاثة:

1/القبول المباشر Accept cookies .

2/طلب الأذن منك Ask me before accept cookies.

3/إبطال فعلها Disable cookies.

أيضا هناك ما يسمى برمجيات جافا (وجافا سكريبت واكتف اكس) حيث يمكن تحت ظروف معينة ان يتمكن الموقع من الحصول علي عنوان بريدك الإلكتروني واسمك الحقيقي وبعض المعلومات الأخرى بواسطة هذه البرمجيات. لكنك تستطيع شل عمل جافا في متصفحك اكسبلورر كالتالي :-

-اختر Internet options من viewو tools

-اختر لسان التبويب advancedوحرك الزالق للأسفل حتي يصل للخيار Java وأزل علامتي الاختيار (التمكين) من مربعي:

Enable Java JIT compiler

Enable Java logging

وكذلك بالنسبة ل Active x يمكنك اتباع ما يلي :

-اختر لسان التبويب Security من Internet options وانقر على الزر Custom level فيظهر مربع حوار ...انقر على الزر Settings فيظهر مربع آخر ..حرك الزالق للأسفل وعند الأمر Download unsigned Active X controls اختر الخيار Disable لعدم التمكين. كذلك في أسفل مربع الحوار هذا عند الفقرة Reset to اختر الخيار : Medium security

ملاحظة 1:اذا اردت معرفة المزيد من المعلومات حول ما يعرف عنك الاخرون قم بزيارة المواقع التالية:

www.privacy.net/analyze
www.privacy.net/anonymizer
www.thematrix.com
www.consumer.net/analyze

ملاحظة 2: المواقع التالية هي مجمل المواقع التي تقدم لك خدمة الامان على الانترنت :

www.anonymizer.com
www.privacyx.com
www.zeroknowledge.com
www.privacy.net/software
www.webtrends.net/tools/security/scan.asp
www.ziplip.com
www.verisign.com
www.nai.com
www.sterlingweb.com
www.dbsecure.com
www.dir.yahoo.com/Business_and_economy/Companies/Computers/security/Software/encryption
www.cs.berkley.edu/~raph/remailer-list.html
www.lockdown2000.com
www.q8kiss.com

